IN THE CLAIMS:

No amendments to the claims are being made.

1. (Previously Presented) A method for protecting digital image files distributed over a network, comprising:

receiving a request from a client computer running a network browser, for an original layout page containing references to digital image files therein;

parsing the original layout page for references to digital image files that are designated as being protected;

generating a modified layout page from the original layout page by replacing at least one of the references to digital image files in the original layout page that are designated as being protected, with references to corresponding encrypted digital image files, prior to responding to the client computer request; and

sending the modified layout page to the client computer in response to the client computer request.

2. (Original) The method of claim 1 wherein the layout page is a hyper-text markup language (HTML) page.

3. (Original) The method of claim 1 wherein the layout page is an extended markup language (XML) page.

4. (Original) The method of claim 1 wherein the layout page is an active server page (ASP).

5. (Previously Presented) The method of claim 1 further comprising determining characteristics of the network browser used by the client computer to issue the request.

6. (Previously Presented) The method of claim 5 wherein the types of substitute data files referenced in the modified layout page depend on the characteristics of the network browser used by the client computer.

7. (Previously Presented) The method of claim 1 wherein said parsing comprises:

locating tags within the layout page indicating references to digital image files; and

identifying protection status of the digital image files, based on information in a protection status database.

8. (Previously Presented) The method of claim 1 wherein said parsing comprises:

locating tags within the layout page delimiting protected parts of the layout page;

extracting references to digital image files within the protected parts of the layout page; and

identifying protection status of the digital image files, based on information in a protection status database.

9. (Previously Presented) The method of claim 1 wherein the substitute data files are pre-defined data files.

10. (Previously Presented) The method of claim 9 wherein the pre-defined data files are pre-defined text files.

11. (Previously Presented) The method of claim 9 wherein the pre-defined data files are pre-defined digital image files.

12. (Previously Presented) The method of claim 1 further comprising deriving the substitute data files from the digital image files.

13. (Previously Presented) The method of claim 12 wherein the substitute data files include watermarked images derived from the digital image files.

14. (Previously Presented) The method of claim 12 wherein the substitute data files include encrypted data derived from the digital image files using an encryption algorithm.

15. (Previously Presented) The method of claim 1 wherein at least one of the references to digital image files is a reference to an alias for a protected digital image file name.

16. (Previously Presented) The method of claim 15 further comprising looking up a file name for the protected digital image file, corresponding to the alias for the protected digital image file name.

17. (Previously Presented) The method of claim 15 wherein the protected digital image file resides on a remote computer.

18. (Previously Presented) The method of claim 17 further comprising looking up an address for the remote computer and a file name for the protected digital image file, corresponding to the alias for the protected digital image file name.

19. (Previously Presented) The method of claim 18 further comprising:

requesting a protected digital image file from the remote computer, using the address for the remote computer and the file name for the protected digital image file; and

receiving a protected digital image file from the remote computer.

20. (Previously Presented) The method of claim 19 further comprising deriving the substitute data file from the protected digital image file.

21. (Previously Presented) The method of claim 20 wherein the substitute data file includes a watermarked image derived from the protected digital image file.

22. (Previously Presented) The method of claim 20 wherein the substitute data file includes encrypted data derived from the protected digital image file using an encryption algorithm.

23. (Previously Presented) A system for protecting digital image files distributed over a network, comprising:

a receiver receiving a request from a client computer running a network browser, for an original layout page containing references to digital image files therein;

a layout page parser parsing the original layout page for references to digital image files that are designated as being protected;

a layout page generator generating a modified layout page from the original layout page by replacing at least one of the references to digital image files in the original layout page that are designated as being protected, with references to corresponding encrypted digital image files, prior to responding to the client computer request; and

a transmitter sending the modified layout page to the client computer in response to the client computer request.

24. (Original) The system of claim 23 wherein the layout page is a hyper-text markup language (HTML) page.

25. (Original) The system of claim 23 wherein the layout page is an extended markup language (XML) page.

26. (Original) The system of claim 23 wherein the layout page is an active server page (ASP).

27. (Original) The system of claim 23 further comprising a browser detector determining characteristics of the network browser used by the client computer to issue the request.

28. (Previously Presented) The system of claim 27 wherein the substitute data files referenced in the modified layout page depend on the characteristics of the network browser used by the client computer.

29. (Previously Presented) The system of claim 23 wherein said layout page parser comprises:

a tag locator locating tags within the layout page indicating references to digital image files; and

a protection status detector identifying protection status of the digital image files, based on information in a protection status database.

30. (Previously Presented) The system of claim 23 wherein said layout page parser comprises:

a tag locator locating tags within the layout page delimiting protected parts of the layout page;

a digital image detector extracting references to digital image files within the protected parts of the layout page; and

a protection status detector identifying protection status of the digital image files, based on information in a protection status database.

31. (Previously Presented) The system of claim 23 wherein the substitute data files are pre-defined data files.

32. (Previously Presented) The system of claim 31 wherein the pre-defined data files are pre-defined text files.

33. (Previously Presented) The system of claim 31 wherein the pre-defined data files are pre-defined image files.

34. (Previously Presented) The system of claim 33 further comprising a data processor deriving substitute data files from the digital image files.

35. (Previously Presented) The system of claim 34 wherein the substitute data files include watermarked images derived from the digital image files.

36. (Previously Presented) The system of claim 34 wherein the substitute data files include encrypted data derived from the digital image files using an encryption algorithm.

37. (Previously Presented) The system of claim 23 wherein at least one of the references to digital image files is a reference to an alias for a protected digital image file name.

38. (Previously Presented) The system of claim 37 further comprising a file name index containing a file name for the protected digital image file corresponding to the alias for the protected digital image file name.

39. (Previously Presented) The system of claim 37 wherein the protected digital image file resides on a remote computer.

40. (Previously Presented) The system of claim 39 further comprising an address and file name index containing an address for the remote computer and a file name for the protected digital image file, corresponding to the alias for the protected digital image file name.

41. (Previously Presented) The system of claim 40 wherein said transmitter requests the protected digital image file from the remote computer, using the address for the remote computer and the file name for the protected digital image file, and wherein said receiver receives the protected digital image file from the remote computer.

42. (Previously Presented) The system of claim 41 further comprising a data processor deriving a substitute data file from the protected digital image file.

43. (Previously Presented) The system of claim 42 wherein the substitute data file includes a watermarked image derived from the protected digital image file.

44. (Previously Presented) The system of claim 42 wherein the substitute data file includes encrypted data derived from the protected digital image file using an encryption algorithm.

45. (Previously Presented) A method for protecting digital image files distributed over a network, comprising:

receiving a request from a client computer;

submitting the request to a server computer;

receiving an original layout page containing references to digital image files therein from the server computer;

parsing the original layout page for references to digital image files that are designated as being protected;

generating a modified layout page from the original layout page by replacing at least one of the references to digital image files in the original layout page that are designated as being protected, with references to corresponding encrypted digital image files, prior to responding to the client computer request; and

sending the modified layout page to the client computer in response to the client computer request.

46. (Previously Presented) The method of claim 45 further comprising:

appending an identifier to the request;

authenticating the request based on the identifier; and

removing the identifier from the request.

47. (Previously Presented) The method of claim 46 further comprising randomly generating the identifier.

48. (Previously Presented) The method of claim 45 further comprising dynamically generating the original layout page.

49. (Original) The method of claim 45 wherein the layout page is a hyper-text markup language (HTML) page.

50. (Original) The method of claim 45 wherein the layout page is an extended markup language (XML) page.

51. (Original) The method of claim 45 wherein the layout page is an active server page (ASP).

52. (Previously Presented) The method of claim 45 wherein said parsing step comprises:

locating tags within the layout page indicating references to digital image files; and

identifying protection status of the digital image files, based on information in a protection status database.

53. (Previously Presented) The method of claim 45 wherein said parsing comprises:

locating tags within the layout page delimiting protected parts of the layout page;

extracting references to digital image files within the protected parts of the layout page; and

identifying protection status of the digital image files, based on information in a protection status database.

54. (Previously Presented) The method of claim 45 wherein the substitute data files are pre-defined image files.

55. (Previously Presented) The method of claim 45 further comprising deriving the substitute data files from the digital image files.

56. (Previously Presented) The method of claim 55 wherein the substitute data files include watermarked images derived from the digital image files.

57. (Previously Presented) The method of claim 55 wherein the substitute data files include encrypted data derived from the digital image files using an encryption algorithm.

58. (Previously Presented) The method of claim 45 wherein at least one of the references to digital image files is a reference to an alias for a protected digital image file name.

59. (Previously Presented) The method of claim 58 further comprising looking up a file name for the protected digital image file, corresponding to the alias for the protected digital image file name.

60. (Previously Presented) The method of claim 58 wherein the protected digital image file resides on a remote computer.

61. (Previously Presented) The method of claim 60 further comprising looking up an address for the remote computer and a file name for the protected digital image file, corresponding to the alias for the protected digital image file name.

62. (Previously Presented) The method of claim 61 further comprising:

requesting protected a digital image file from the remote computer, using the address for the remote computer and the file name for the protected digital image file; and

receiving the protected digital image file from the remote computer.

63. (Previously Presented) The method of claim 62 further comprising deriving the substitute data file from the protected digital image file.

64. (Previously Presented) The method of claim 63 wherein the substitute data file includes a watermarked image derived from the protected digital image file.

65. (Previously Presented) The method of claim 63 wherein the substitute data file includes encrypted data derived from the protected digital image file using an encryption algorithm.

66. (Previously Presented) A system for protecting digital image files distributed over a network, comprising:

a receiver receiving a request from a client computer and receiving an original layout page containing references to digital image files therein from a server computer;

a transmitter submitting the request to the server computer, and sending a modified layout page to the client computer in response to the client computer request;

a layout page parser parsing the original layout page for references to digital image files that are designated as being protected; and

a layout page generator generating the modified layout page from the original layout page by replacing at least one of the references to digital image files in the original layout page that are designated as being protected, with

references to corresponding encrypted digital image files, prior to responding to the client computer request.

67. (Original) The system of claim 66 further comprising:

a request modifier appending an identifier to the request and removing the identifier from the request; and

a request authenticator authenticating the request based on the identifier.

68. (Original) The system of claim 67 further comprising an identifier generator randomly generating the identifier.

69. (Original) The system of claim 66 further comprising an interpreter dynamically generating the original layout page.

70. (Original) The system of claim 66 wherein the layout page is a hyper-text markup language (HTML) page.

71. (Original) The system of claim 66 wherein the layout page is an extended markup language (XML) page.

72. (Original) The system of claim 66 wherein the layout page is an active server page (ASP).

73. (Previously Presented) The system of claim 66 wherein said layout page parser comprises:

a tag locator locating tags within the layout page indicating references to digital image files; and

a protection status detector identifying protection status of the digital image files, based on information in a protection status database.

74. (Previously Presented) The system of claim 66 wherein said layout page parser comprises:

a tag locator locating tags within the layout page delimiting protected parts of the layout page;

a digital image detector extracting references to digital image files within the protected parts of the layout page; and

a protection status detector identifying protection status of the digital image files, based on information in a protection status database.

75. (Previously Presented) The system of claim 66 wherein the substitute data files are pre-defined image files.

76. (Previously Presented) The system of claim 66 further comprising a data processor deriving substitute data files from the digital image files.

77. (Previously Presented) The system of claim 76 wherein the substitute data files include watermarked images derived from the digital image files.

78. (Previously Presented) The system of claim 76 wherein the substitute data files include encrypted data derived from the digital image files using an encryption algorithm.

79. (Previously Presented) The system of claim 66 wherein at least one of the references to digital image files is a reference to an alias for a protected digital image file name.

80. (Previously Presented) The system of claim 79 further comprising a file name index containing a file name for the protected digital image file corresponding to the alias for the protected digital image file name.

81. (Previously Presented) The system of claim 79 wherein the protected digital image file resides on a remote computer.

82. (Previously Presented) The system of claim 81 further comprising an address and file name index containing an address for the remote computer and a file name for the protected digital image file, corresponding to the alias for the protected digital image file name.

83. (Previously Presented) The system of claim 82 wherein said transmitter requests the protected digital image file from the remote computer, using the address for the remote computer and the file name for the protected digital image file, and wherein said receiver receives the protected digital image file from the remote computer.

84. (Previously Presented) The system of claim 83 further comprising a data processor deriving the substitute data file from the protected digital image file.

85. (Previously Presented) The system of claim 84 wherein the substitute data file includes a watermarked image derived from the protected digital image file.

86. (Previously Presented) The system of claim 84 wherein the substitute data file includes encrypted data derived from the protected digital image file using an encryption algorithm.